Catastrophic Incident Annex

Tab I:
Operational Communication

Catastrophic Incident Annex (CIA)

Tab I: Operational Communication

Table of Contents

Tab I: Operational Communication

Purpose

The purpose of this tab is to describe the delivery of the Operational Communications core capability during a catastrophic incident response. Operational Communication is the means by which all levels of government develop and utilize interoperable voice, video, data systems, and networks essential for operational coordination and effective response operations. The priority of Operational Communications is to provide emergency response resources with mission-critical communication systems and interoperable communications.

Strategic Goals

Life Safety

Vertical Integration

- Establish sufficient communication to enable timely and coordinated assistance to local jurisdictions.
- Establish a shared situational awareness and understanding of the communications operating environment.
- Integrate state-owned and private sector communications equipment with local jurisdictional communications systems to facilitate interoperable communications between the state and local response resources.

Horizontal Integration

- Establish or reestablish communication systems between state agencies, private sector entities, critical infrastructure sectors, and other responding organizations to facilitate operational coordination.

Incident Stabilization

Direction, Control, and Coordination

- Coordinate operational communications response planning among whole community partners.
- Provide State Emergency Operations Center responders with mission-critical communications systems.
- Monitor for communications support requests aimed at providing support for essential services.
- Identify infrastructure barriers preventing the reestablishment or sustainment of communications systems and functionality.
- Establish primary, alternate, contingent, and emergency (PACE) backup communications capabilities and share the status of an agency's capabilities with partner organizations.

Situation Overview

General

Operational Communication is an interconnected interagency system of communications capabilities across all levels of government to provide mission-critical information, operational coordination, and situational awareness vital to disaster responder command and control decision making. Operational Communication plays a direct role in the successful outcome of a response to a catastrophic incident. When communications are not interoperable, are degraded, or unavailable, the ability to perform operational coordination is greatly hindered.

Figure 1 attempts to illustrate the complexity in communications involved in disaster response operations and highlights the need to establish and maintain both multiple communications options and interoperability between those systems. The example below does not include all potential pathways.

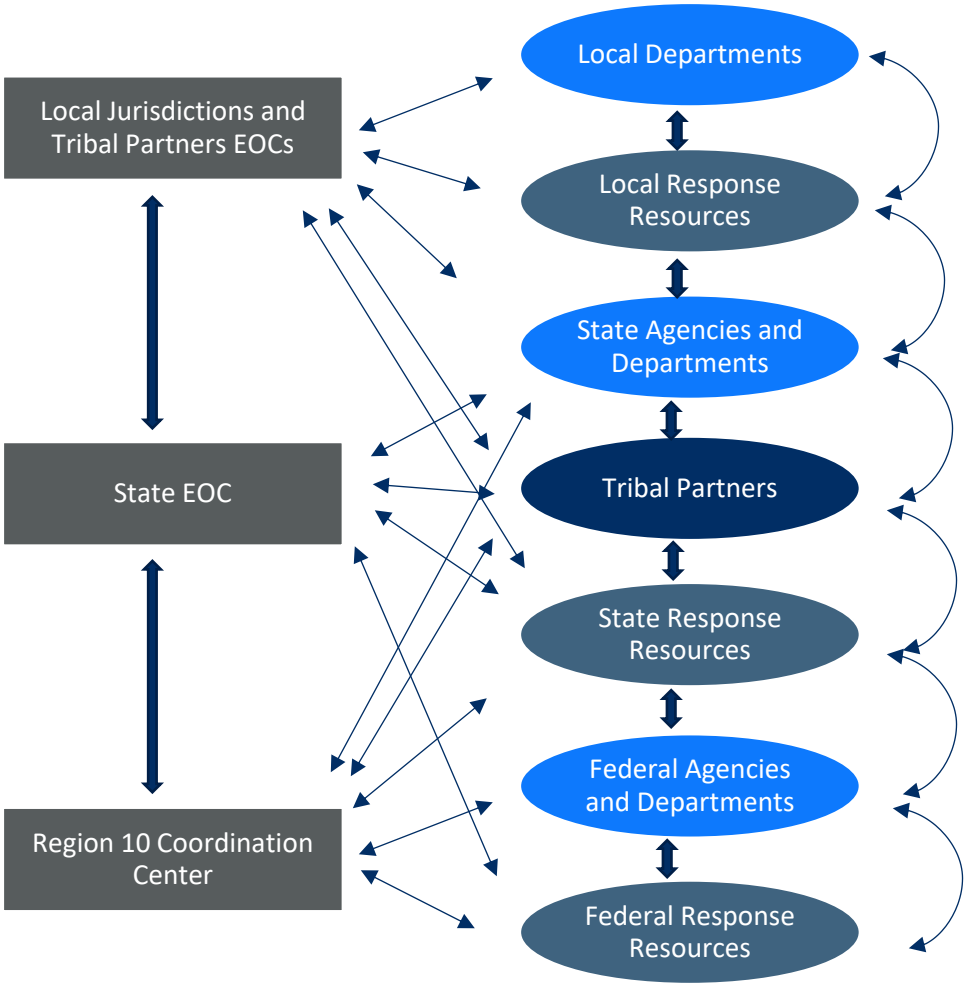

Figure 1 – Example Response Communications Pathways

Tab I: Operational Communication

Operational Communication tools include both hardware and software capabilities required to establish and sustain a disaster response which integrates the whole community. The Operational Communications foundation is based on the ability to process and share timely, dynamic, and reliable information and situational assessments across all levels of government.

Security and Confidentiality

Some catastrophic incidents may highlight an increased need for or enhanced of communications security practices. Communications Security (COMSEC) refers to the security of any information that is transmitted, transferred, or communicated. COMSEC are measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. According to the National Emergency Communications Plan, "as emergency communication systems and functions become more interconnected, they also become more susceptible to physical and cyber vulnerabilities and disruptions in other parts of the Operational Communications Ecosystem."

COMSEC Security Types

- Emission Security (EMSEC): Prevents the release or capture of emanations from equipment, such as cryptographic equipment, thereby preventing unauthorize interception.
- Cryptosecurity: encrypts data, rendering it unreadable until the data is decrypted.
- Physical Security: ensures the safety of, and prevents unauthorized access to, cryptographic information, documents, and equipment.
- Traffic-Flow Security: hides messages and message characteristics flowing on a network.
- Transmission Security (TRANSEC): protects transmissions from unauthorized access, thereby preventing interruption and harm.

Interoperability

The ability for response resources at all levels to respond and stabilize emergency situations relies heavily on the ability to communicate. Interoperability is when emergency responders can work seamlessly with other systems or products without any special effort. Communications interoperability means sharing information via voice and data signals on demand, in real time, when needed, and as authorized. Communications interoperability makes it possible for emergency response agencies to work effectively together and perform effective operational coordination when responding to catastrophic accidents or disasters.

Priorities

A catastrophic incident that requires a multi-agency, multi-jurisdiction response could result in communication system capacity disruptions. If capacity is needed, there may be a need to

prioritize talkgroup or channel users. In developing this priority list, it will be important to identify which systems provide the most support to life saving and life sustaining response operations.

For catastrophic planning, it is important to prioritize those systems that:

1. Provide resource support for local and tribal governments
2. Allow information sharing
3. Support response operational coordination.

Other system usage, while important, would need to be delayed if communication capacity is hindering the top priorities from performing to the standards needed to save and sustain life.

Prioritization will become especially important as an organization moves down their Continuity of Operations Communication PACE (Primary, Alternate, Contingent, and Emergency Communication) plan. Moving from the Primary Communication System to the Alternate, Contingent, and Emergency Systems could potentially decrease system capacity and therefore require prioritization of response operations.

Dependencies

Communications systems are complex and often owned and operated by commercial vendors and carriers leaving public safety responders reliant on those outside parties. The collaboration between agencies sponsoring or owning the public safety communications systems and external entities providing infrastructure or services comes with its own challenges, complexities, and opportunities. To build resilience into operational communications it is important to understand communications infrastructure dependencies and interdependencies, identify potential obstacles to service provider continuity of operations, establish a backup plan, and continue to build relationships and coordinate with key personnel in adjacent or regional jurisdictions.

Considerably more work is needed to understand the communications infrastructure dependencies and interdependencies, to identify potential obstacles to service provider continuity of operations, and to establish backup plans.

WebEOC

Washington State Emergency Operations Center uses WebEOC, an electronic Web-based means of communication between county partners and the state's Emergency Operations Center. The system allows for continual communication of the ongoing situation and reporting and provides a means for requesting and tracking resources.

Planning Assumptions and Response Considerations

General

- Responders and survivors in heavily impacted areas may not have access to modern means of communication; there will be no internet, cell phone, landline, television, or two-way radio service.
- Restoration of communications capabilities which support or enable the primary core capabilities is essential to incident response.
- Communications may be cut off completely in isolated areas and communities and will require direct contact.
- Critical infrastructure interdependencies among the communications, electricity, fuel, and transportation sectors will significantly impact the ability to deploy temporary solutions within the affected areas for the initial life-safety response.
- Damage to interdependent communications systems (land line, cell tower, radio towers, and microwave) will affect restoration of all critical infrastructure sectors and hamper situational awareness.
- Lack of communications and impaired accessibility to impacted areas may limit situational assessment.
- Satellite and radio frequencies (RF), including amateur radio networks, may be the primary communications modes in the affected areas.
- Debris and road damage will prevent access to communications towers, central offices, remote switches, cable head-ends, and other critical communications infrastructure to assess damages, to conduct repair operations, and for the refueling of generators.
- Wireline (copper and fiber) systems may be damaged by debris removal, cleanup, and repair operations as active communications links—both overhead and underground—get damaged or even severed.
- Infrastructure damage in western regions of the state will affect communications in eastern regions (and vice versa).
- Following disruptions to communication systems, communications may continue to deteriorate for 8–12 hours following the incident due to the loss of backup power, fuel, etc.
- Demand on communications networks may cause congestion, resulting in latency, call failures, or other communications issues. Communications priority systems, such as the Government Emergency Telephone System (GETS) and the Wireless Priority Service (WPS), help alleviate issues for responders and other officials.
- Trunked radio systems may be degraded or inoperable due to failures with copper, fiber, and microwave transmission modes.
- Cellular towers may not be able to link customers to switching centers, leaving customers with no access to emergency and telecommunications service.

- A significant amount of communications infrastructure depends on commercial heating, cooling, water (HVAC), and power to operate.
- Responders may have limited information about surviving communications infrastructure as well as assets that require restoration.
- Some physical communications infrastructure may fail or become destroyed during the incident and disable one or more methods of communication
- Some communication infrastructure sites are in difficult to reach locations and require special transportation capabilities to access to repair or refuel
- Bringing in telecommunications crews and resources from unaffected areas requires significant coordination and can be complicated by infrastructure conditions.
- Damage to interdependent communications systems (landline, cell tower, radio tower, and microwave) affects restoration of all critical infrastructure sectors and hampers situational awareness.
- Communications restoration equipment (generators, fuel tanks, cabling) and existing infrastructure are at risk of theft and vandalism.
- Overuse of communications networks may cause congestion, resulting in latency, call failures, or other communications issues. Communications priority systems, such as the Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS), help alleviate issues for responders and other officials.

Power

- Commercial carriers may not have adequate backup power for some cell sites and may rely solely on battery power in some instances.
    - With no commercial power available, radios would have to be battery operated, and use both rechargeable and disposable batteries available on the local market.
- Power needs for commercial partners may not be identified as a priority for route clearance, access to generators, or refueling, which may make prioritizing response difficult.
- A significant amount of communications infrastructure depends on commercial heating, ventilation and air-conditioning (HVAC), and power to operate, which may not be functioning within impacted areas with significant damage to energy infrastructure.

Backup Communications

- There may be a need to develop a communication precedence or an order in which a response organization will move through available communications systems until contact is established.
- Agency contract vendors have developed their own business continuity plans and disaster recovery plans and can guarantee reconstitution of their systems within a certain time frame.

Capability Targets

- *Within (#) (time) of an incident, establish interoperable communications across (#) jurisdictions affected and with (#) partner organizations involved in incident management. Maintain for (#) (time).*

Non-Standardized Targets

- *Within (#) (time) of an incident, assess the status of (#) state emergency operations center communication systems to receive and send information to (#) jurisdictions.*
- *Within (#) (time) of an incident, re-establish SEOC communication to external partners through utilization of the Primary, Alternate, Contingent, and Emergency systems, and relay the status of SEOC communication systems to (#) local jurisdictions.*
- *Within (#) (time) of an incident, gather assessment information on the status of jurisdiction communication systems to receive and send incident information.*
    - *Including contacting (#) Public Safety Answering Points if local jurisdiction EOCs are unreachable within (#) (time) of incident or loss of communication.*
- *Within (#) (time) of an incident, assist local jurisdictions in the establishment of two way communication between the SEOC and jurisdiction.*

Concept of Operations

General

PACE and Communications COOP

As mentioned in the Situation Overview portion of this Tab, an organization's PACE or their Primary, Alternate, Contingent, and Emergency communication systems or methodologies are essential to the continuity of operations during a catastrophic response. It is necessary for local, state, federal, Tribal, critical infrastructure, and private sector and business organizations to develop a robust communications continuity plan. Communication continuity will be necessary for all other aspects of response, especially Operational Coordination, Situational Assessment,

and Logistics and Supply Chain Management. Every Core Capability relies on consistent, reliable communication.

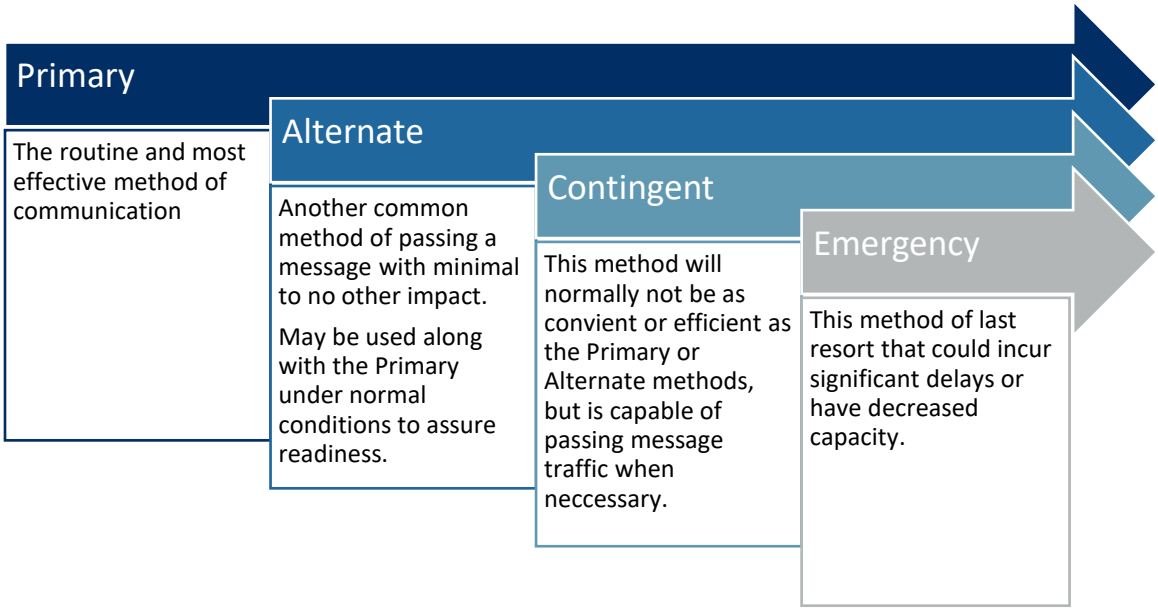

Figure 2 - Primary, Alternate, Contingency, and Emergency (PACE) Communications Process

Local Integration into PACE

One of the challenges in changing from one communication method to another is getting other responders the information about which mode is being used. If your organization is utilizing the primary system, yet another organization has already moved down their PACE and is utilizing their contingent or emergency system, communication interoperability becomes a key priority. For example, response communications will need to consider how a local jurisdiction will notify the SEOC that they are now utilizing their Alternate, Contingent, or Emergency communication system and concurrently, how the SEOC will notify all local jurisdictions that they are utilizing their Alternate, Contingent, or Emergency form of communication.

Supporting Core Capability

Operational Communication

Objective:

Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impacted area and all response forces.

Critical Tasks:

1. Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between Federal, tribal, state, and local first responders.
2. Re-establish sufficient communications infrastructure within the affected areas to support ongoing life-sustaining activities, provide basic human needs, and a transition to recovery.
3. Re-establish critical information networks, including cybersecurity information sharing networks, to inform situational awareness, enable incident response, and support the resilience of key systems.

Direction, Control, and Coordination

Horizontal Integration

Alert & Warning Center

The Alert and Warning Center (A&WC) within the State Emergency Operations Center has direct contact with the regional, city, county PSAPs for Washington. Communication through the Alert and Warning Center about the status of a jurisdictions communication systems and what method they are communicating with will be essential for mission response.

Vertical Integration

Public Safety Answering Points

Public Safety Answering Points (PSAPs) are the gateways for access to emergency services for the public. PSAP operators are also often the first link that emergency management may have to the incident that is occurring in their community.

In the event of loss of communication between the local emergency operations center and the state emergency operations center, the Public Safety Answer Points could become a relay for the PACE communications to link local and state EOCs. It will be

Figure 3: If first responders are the eyes to the incidents happening on the scene of an incident, or disaster, Public Safety Answering Points (PSAPs) are the ears. These Emergency Communication Centers gather the on-scene reports by residents, responders, and by-standers and relay that information to appropriate responders and the Local Emergency Operations Center if warranted.

essential for the SEOC to know how a local jurisdiction is communicating so that incident response can be supported.

Information Collection, Analysis, & Dissemination

Information Collection

Operational Communications enables the Information Collection, Analysis, & Dissemination through Community Lifeline Reporting. It is not enough to collect data alone. Data must be analyzed and converted into useful and actionable information through analysis, and this information needs to be shared through dissemination.

General Essential Elements of Information (EEIs)

Community Lifeline	Lifeline Component	Lifeline Subcomponent	Essential Element of Information
All	All	All	• Immediate resource needs for communication systems essential for the implementation of life safety and life sustainment response within each community lifeline sector. • Availability and functionality of response communication primary, alternate, contingent, and emergent systems used for communication. • Availability of response resources to meet the communication system needs identified for each community lifeline sector. • Immediate resource needs for communication with local jurisdiction communication systems.
Communications	Infrastructure	Data Centers	• Availability of network or data centers resilient to power loss. • Systems assets available to restore service if there is an outage. ○ Regulations and costs to deploying those assets. • Who controls the installation of infrastructure components and subscriber equipment?

			• Who holds the FCC licenses for shared systems? • Does an MOU exist that authorizes the use of the shared system?
	Responder Communications	LMR Networks	• If capacity is needed, how are lower priority users moved off the designated interoperability talkgroup(s) or channel(s)?
	Alerts, Warnings, and Messages	Local Alert/ Warning Ability Access to IPAWS (WEA, EAS, NWR) NAWAS Terminals	• Status of local alert and warning ability • Access to Integrated Public Alert & Warning System (IPAWS) • Access to Wireless Emergency Alert (WEA) • Access to Emergency Alert System (EAS) • NOAA Weather Radio (NWR) • National Warning System (NAWAS) terminals

Information Analysis

All ESFs and response operations share a relationship with Operational Communications. Information collected through impacts to Community Lifelines should be analyzed by ESFs to inform new or ongoing response objectives which involvement the identification, request for, or movement of resources.

Information Dissemination

Information analysis will result in contributions to the Tier 1: Disaster Summary, Senior Leadership Brief (SLB) provided to the UCG. Additionally, the more detailed information not necessary for executive level response decision making will be supplied for the creation of the Tier 2: Lifeline Overview SLB for use in tracking conditions and informing response personnel.

Responsibilities

Phase 1 (Prepare)

Phase 1	
Operational Communications	Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impacted area and all response forces.

SEOC

- Maintain and update, exercise and evaluate the Emergency Support Function 2 plan and this Operational Communication Tab to the CIA.
- Build and sustain partnerships with critical communication partners involved in the planning and response during a communications failure. Horizontal involvement in the development of communication systems planning to increase interoperability.
- Development of technical voice and data standard operating procedures to prevent incompatible technology from communication equipment vendors.
- As part of COOP planning, identify critical IT systems, communication systems, and dependencies and determine their order of priority for protection and restart.
- Ensure system backups are established and operational.
- Identify, understand, and monitor power dependencies and redundancies
- Establish network redundancy by utilizing multiple resilient networks

ESF 2

- As part of planning, training, and exercises, establish action plans to include contacting commercial partners directly to locate commercial power disruptions and enable prioritization of aid to ensure power resiliency
- Work with commercial partners before and during an incident to identify and understand power resiliency weaknesses
- Establish relationships with commercial partners in advance so that major assets affected can be located and accessed quickly
- Establish network redundancy by utilizing multiple resilient networks
- Establish multiple backup systems for power (e.g., generators and battery power) and communication (e.g., buried fiber lines or other wireline connections, microwave backhaul)
- Designation of specific response organizations to maintain operational control of their own communications systems, while coordinating with the EOC during emergency operations.
- Train with ham radio operators, radio clubs, and private organizations with sophisticated communications equipment.

Phase 2 (Initial Response, Employment of Resources, Transition to Recovery)

Phase 2a, 2b, 2c	
Operational Communications	Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impacted area and all response forces.

SEOC

- Identify communications requirements for internal and external stakeholders, local jurisdictions, and other response partners across the whole community.
- Rebuild and/or reestablish EMD networks post-incident.
- Restore EMD system data from established backups.
- Restore communication for the SEOC with established or backup network providers.
- Coordinate the assessment of local jurisdiction communication status.
- Deliver information on the current status of SEOC communication systems to local jurisdictions
  - If direct communication to the local jurisdiction EOC is unavailable, assess the utilization of Public Safety Answering Points as a relay for communications.
- Provide communications capabilities for SEOC Representatives and other Field Forces.
- Prepare demobilization and transition plan to ensure restoration efforts continue.

Alert & Warning Center

- If necessary, relay the status of the SEOC PACE communications status to the local, regional, or city PSAPs so interoperable communication can occur.

ESF 2

- Setup and test portable network devices to provide communications between sections and ESF partners, policy group and elected officials.
- Assess potential field personnel and facility communications requirements
- Source mobile communications capability for isolated communities and other state identified priorities.

References and Supporting Guidance

National Emergency Communications Plan (NECP)
The NECP establishes a vision to enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event.

Public Safety Communications Dependencies on Non-Agency Infrastructure and Services
The purpose of this white paper is to help system administrators, public administration decision makers, and other stakeholders involved in public safety communications identify non-agency dependencies that should be considered during system lifecycle planning and implementation.

Task Force on Optimal PSAP Architecture, Final Report
The FCC's Task Force on Optimal Public Safety Answering Point (PSAP) Architecture (Task Force or TFOPA) was directed to study and report findings and recommendations on structure and architecture in order to determine whether additional consolidation of PSAP infrastructure and architecture improvements would promote greater efficiency of operations, safety of life, and cost containment, while retaining needed integration with local first responder dispatch and support.

Washington Statewide Communications Interoperability Plan
The Washington Statewide Communications Interoperability Plan (SCIP) is a stakeholder-driven, multijurisdictional, and multi-disciplinary strategic plan to enhance interoperable and emergency communications over the next one to three years.

Terms and Definitions

COMSEC
A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material.

Interoperability
The ability of emergency response agencies to talk to one another via communication systems – to exchange voice and/ or data with one another on demand, in real time, when needed, and as authorized.

Shared System
A system used by multiple agencies and multiple jurisdictions (e.g., statewide, regional, or county radio systems) where radios communicate with each other over a common infrastructure using the standards-based system of systems approach.